

ON SEMIGROUPS WITH PSPACE-COMPLETE SUBPOWER MEMBERSHIP PROBLEM

MARKUS STEINDL

ABSTRACT. Fix a finite semigroup S and let a_1, \dots, a_k, b be tuples in a direct power S^n . The subpower membership problem (SMP) for S asks whether b can be generated by a_1, \dots, a_k . For combinatorial Rees matrix semigroups we establish a dichotomy result: if the corresponding matrix is of a certain form, then the SMP is in P; otherwise it is NP-complete. For combinatorial Rees matrix semigroups with adjoined identity, we obtain a trichotomy: the SMP is either in P, NP-complete, or PSPACE-complete. This result yields various semigroups with PSPACE-complete SMP including the 6-element Brandt monoid, the full transformation semigroup on 3 or more letters, and semigroups of all n by n matrices over a field for $n \geq 2$.

1. INTRODUCTION

In this paper we continue the investigation of the subpower membership problem (SMP) for semigroups started in [1] and [10]. At the Conference on Order, Algebra, and Logics in Nashville, 2007, Ross Willard proposed the SMP as follows [12]: Fix a finite algebraic structure S with finitely many basic operations. Then the *subpower membership problem* for S is the following decision problem:

SMP(S)

Input: $\{a_1, \dots, a_k\} \subseteq S^n, b \in S^n$

Problem: Is b in the subalgebra of S^n generated by a_1, \dots, a_k ?

The SMP occurs in connection with the constraint satisfaction problem (CSP) [4]. In the algebraic approach to the CSP, each constraint relation is considered to be a subalgebra of a power (*subpower*) of a certain finite algebra whose operations are the polymorphisms of the constraint language. Checking whether a given tuple belongs to a constraint relation represented by its generators is precisely the SMP for the polymorphism algebra.

The input size of SMP(S) is essentially $(k+1)n$. We can always decide the problem using a straightforward closure algorithm in time exponential in n . Thus SMP(S) is in EXPTIME for every algebra S . However, the following questions arise:

- How does the algebra S affect the computational complexity of SMP(S)?
- For which algebras S can SMP(S) be solved in time polynomial in k and n ?

Date: April 8, 2016.

2000 Mathematics Subject Classification. Primary: 20M99; Secondary: 68Q25.

Key words and phrases. subalgebras of powers, membership test, computational complexity, PSPACE-complete, NP-complete.

Supported by the Austrian Science Fund (FWF): P24285.

- When is the problem complete in NP, PSPACE, or EXPTIME? Can it also be complete in a class other than these?

Mayr [6] proved that the SMP for Mal'cev algebras is in NP. He also showed that for certain generalizations of groups and quasigroups the SMP is in P. Kozik [5] constructed a finite algebra with EXPTIME-complete SMP.

For semigroups the SMP is in PSPACE. This was shown in [1] by Bulatov, Mayr, and the author of the present paper. We also proved that the SMP of the full transformation semigroup on five letters is PSPACE-complete. It was the first algebra known to have a PSPACE-complete SMP. In the same paper a dichotomy result for commutative semigroups was established: if a commutative semigroup S embeds into a direct product of a Clifford semigroup and a nilpotent semigroup, then $\text{SMP}(S)$ is in P; otherwise it is NP-complete.

Another dichotomy for idempotent semigroups was established in [10]: if an idempotent semigroup S satisfies a certain pair of quasiidentities, then $\text{SMP}(S)$ is in P; otherwise it is NP-complete.

The first result of the current work is a condition for a semigroup S under which $\text{SMP}(S)$ is NP-hard:

Theorem 1.1. *Let r, s, t be elements of a finite semigroup S such that s does not generate a group and $rs = st = s$. Then $\text{SMP}(S)$ is NP-hard.*

We will prove this result in Section 2 by reducing the Boolean satisfiability problem SAT to $\text{SMP}(S)$.

A semigroup is called *combinatorial* if every subgroup has one element. Combinatorial *Rees matrix semigroups* are of the form $\mathcal{M}^0(\{1\}, I, \Lambda, P)$ (see [3, Theorem 3.2.3]). We give the following alternative notation: For nonempty sets I, Λ and a matrix $P \in \{0, 1\}^{\Lambda \times I}$ we let $S_P := (I \times \Lambda) \cup \{0\}$ and define a multiplication on S_P by

$$[i, \lambda] \cdot [j, \mu] := \begin{cases} [i, \mu] & \text{if } P(\lambda, j) = 1, \\ 0 & \text{if } P(\lambda, j) = 0, \end{cases}$$

$$0 \cdot [i, \lambda] := [i, \lambda] \cdot 0 := 0 \cdot 0 := 0.$$

It is easy to see that S_P is indeed a combinatorial semigroup. We say the matrix $P \in \{0, 1\}^{\Lambda \times I}$ has *one block* if there exist $J \subseteq I$, $\Delta \subseteq \Lambda$ such that for $i \in I$, $\lambda \in \Lambda$,

$$P(\lambda, i) = 1 \quad \text{if and only if} \quad (\lambda, i) \in \Delta \times J.$$

For $P = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ we call $B_2 := S_P$ the *Brandt semigroup*, and for $P = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ we denote S_P by A_2 .

In Section 3 we establish the following two results:

Theorem 1.2. *Let S_P be a finite combinatorial Rees matrix semigroup. If the matrix P has one block, then $\text{SMP}(S_P)$ is in P. Otherwise $\text{SMP}(S_P)$ is NP-complete.*

Corollary 1.3. *The SMP for the Brandt semigroup B_2 and for the semigroup A_2 is NP-complete.*

In Section 4 we state a condition for semigroups S under which $\text{SMP}(S)$ is PSPACE-complete:

Theorem 1.4. *Let S be a finite semigroup and $s, t, \underline{1} \in S$ such that*

- (a) $sts = s$,

- (b) s does not generate a group,
- (c) $s\underline{1} = s$ and $t\underline{1} = t$.

Then $\text{SMP}(S)$ is PSPACE-complete.

In the proof we will reduce quantified 3SAT to $\text{SMP}(S)$. It follows that adjoining an identity to B_2 or A_2 already results in a PSPACE-complete SMP:

Theorem 1.5. *The SMP for the Brandt monoid B_2^1 and for the monoid A_2^1 is PSPACE-complete.*

This result is part of Corollary 4.9. Both B_2^1 and A_2^1 embed into T_3 , the full transformation semigroup on three letters. Thus $\text{SMP}(T_3)$ is also PSPACE-complete. So Theorem 1.5 generalizes the result from [1] that $\text{SMP}(T_5)$ is PSPACE-complete. In addition, B_2 and A_2 are the first groupoids known to have an NP-complete SMP where adjoining an identity yields a groupoid with PSPACE-complete SMP. Further examples of semigroups with PSPACE-complete SMP are listed in Section 4.

In Section 5 we will consider Rees matrix semigroups with adjoined identity and prove the following trichotomy result:

Theorem 1.6. *Let S_P be a finite combinatorial Rees matrix semigroup.*

- (a) *If all entries of the matrix P are 1, then $\text{SMP}(S_P^1)$ is in P.*
- (b) *If P has one block and some entries are 0, then $\text{SMP}(S_P^1)$ is NP-complete.*
- (c) *Otherwise $\text{SMP}(S_P^1)$ is PSPACE-complete.*

2. SEMIGROUPS WITH NP-HARD SMP

In this section we will prove Theorem 1.1 by reducing the Boolean satisfiability problem SAT to $\text{SMP}(S)$. It follows that the SMP for a semigroup S is already NP-hard if S has a \mathcal{D} -class that contains both group and non-group \mathcal{H} -classes.

We denote Green's equivalences by $\mathcal{L}, \mathcal{R}, \mathcal{J}, \mathcal{H}, \mathcal{D}$ [3, p. 45]. For the definition of the related preorders $\leq_{\mathcal{L}}, \leq_{\mathcal{R}}, \leq_{\mathcal{J}}$ see [3, p. 47]. We write $[n] := \{1, \dots, n\}$ for $n \in \mathbb{N}$ and set $[0] := \emptyset$. We consider a tuple a in a direct power S^n to be a function $a: [n] \rightarrow S$. This means the i th coordinate of this tuple is denoted by $a(i)$ rather than a_i . The subsemigroup generated by a set $A = \{a_1, \dots, a_k\}$ may be denoted by $\langle A \rangle$ or $\langle a_1, \dots, a_k \rangle$.

Lemma 2.1. *Let s belong to a finite semigroup S . Then s generates a group if and only if $s^2 \mathcal{J} s$.*

Proof. If s generates a group, then $s^k = s$ for some $k \geq 2$. Thus $s^2 \mathcal{J} s$.

For the converse let $s^2 \mathcal{J} s$. First assume the \mathcal{J} -class J_s is the minimal ideal of S . Then J_s is a finite simple semigroup by [3, Proposition 3.1.4]. By the Rees Theorem for finite simple semigroups s generates a group.

Now assume J_s is not the minimal ideal of S . Let

$$J(s) := \{r \in S \mid r \leq_{\mathcal{J}} s\}, \quad I(s) := \{r \in S \mid r <_{\mathcal{J}} s\}.$$

By [3, Proposition 3.1.4] the principal factor $J(s)/I(s)$ is either null or 0-simple. Since $s^2 \mathcal{J} s$, the second case applies. By the Rees Theorem for finite 0-simple semigroups s generates a group. \square

Lemma 2.2. *Let r, s, t be elements of a finite semigroup S such that s does not generate a group and $rs = st = s$. Then there are idempotents $e, f \in S$ such that $es = sf = s$ and every product $a_1 \cdots a_k$ in s, e, f in which s occurs at least twice does not yield s .*

Proof. First assume s is regular, i.e. $sus = s$ for some $u \in S$. Let e and f be the idempotent powers of su and us respectively. Clearly $es = sf = s$. Let $a_1 \cdots a_k$ be a product in s, e, f , and $i < j$ such that $a_i = a_j = s$. Let $\ell \in \{i+1, \dots, j\}$ be maximal such that $a_{i+1} = \dots = a_{\ell-1} = f$. Then $a_i \cdots a_{\ell-1} = s$, and thus $a_i \cdots a_\ell \in \{s^2, se\}$. Note that $se = s(su)^m$ for some $m \in \mathbb{N}$. Now a factor s^2 occurs in the product $a_i \cdots a_\ell$. Since s does not generate a group, Lemma 2.1 implies that $s^2 <_{\mathcal{J}} s$. Thus $a_1 \cdots a_\ell <_{\mathcal{J}} s$, and the result follows.

Now assume s is not regular. By [3, Theorem 3.1.6] the principal factor $J(s)/I(s)$ is null. Let e and f be the idempotent powers of r and t respectively. Let $a_1 \cdots a_k$ be a product in s, e, f , and let $i < j$ such that $a_i = a_j = s$. Then $a_1 \cdots a_i \leq_{\mathcal{J}} s$ and $a_{i+1} \cdots a_k \leq_{\mathcal{J}} s$. Since $J(s)/I(s)$ is null, it follows that $a_1 \cdots a_k <_{\mathcal{J}} s$. \square

Proof of Theorem 1.1. Let S satisfy the assumptions. We reduce the Boolean satisfiability problem SAT to $\text{SMP}(S)$. SAT is NP-complete [2], and we give the following definition:

SAT

Input: Clauses $C_1, \dots, C_m \subseteq \{x_1, \dots, x_k, \neg x_1, \dots, \neg x_k\}$.

Problem: Do truth values for x_1, \dots, x_k exist for which the Boolean formula $\Phi(x_1, \dots, x_k) := (\bigvee C_1) \wedge \dots \wedge (\bigvee C_m)$ is true?

For all $j \in [k]$ we may assume that x_j or $\neg x_j$ occurs in some clause C_i . We define an $\text{SMP}(S)$ instance

$$A := \{a_1^0, \dots, a_k^0, a_1^1, \dots, a_k^1\} \subseteq S^{k+m}, \quad b \in S^{k+m}.$$

Let $e, f \in S$ be idempotents with the properties from Lemma 2.2. Let g be the idempotent power of se . Observe that e and g form a two-element semilattice with $g < e$.

Let $j \in [k]$ and $z \in \{0, 1\}$. For $i \in [k]$ let

$$a_j^z(i) := \begin{cases} f & \text{if } i < j, \\ s & \text{if } i = j, \\ e & \text{if } i > j, \end{cases}$$

and for $i \in [m]$ let

$$a_j^0(k+i) := \begin{cases} g & \text{if } \neg x_j \in C_i, \\ e & \text{otherwise,} \end{cases}$$

$$a_j^1(k+i) := \begin{cases} g & \text{if } x_j \in C_i, \\ e & \text{otherwise.} \end{cases}$$

Let

$$b(i) := s \quad \text{for } i \in [k],$$

$$b(k+i) := g \quad \text{for } i \in [m].$$

We claim that

- (1) the Boolean formula Φ is satisfiable if and only if $b \in \langle A \rangle$.

For the (\Rightarrow) direction let $z_1, \dots, z_k \in \{0, 1\}$ such that $\Phi(z_1, \dots, z_k) = 1$. We show that

- (2) $b = a_1^{z_1} \cdots a_k^{z_k}$.

For $i \in [k]$ we have $a_1^{z_1} \cdots a_k^{z_k}(i) = e^{i-1} s f^{k-i} = s = b(i)$. For $i \in [m]$ the clause $\bigvee C_i$ is satisfied under the assignment $x_1 \mapsto z_1, \dots, x_k \mapsto z_k$. Thus there is a $j \in [k]$ such that $x_j \in C_i$ and $z_j = 1$, or $\neg x_j \in C_i$ and $z_j = 0$. In both cases $a_j^{z_j}(k+i) = g$, and thus $a_1^{z_1} \cdots a_k^{z_k}(k+i) = g = b(k+i)$. This proves (2) and the (\Rightarrow) direction of (1).

For the (\Leftarrow) direction of (1) assume $b = a_{j_1}^{z_1} \cdots a_{j_\ell}^{z_\ell}$ for some $\ell \in \mathbb{N}$, $j_1, \dots, j_\ell \in [k]$, and $z_1, \dots, z_\ell \in \{0, 1\}$. We show that j_1, \dots, j_ℓ are distinct. Suppose $j_p = j_q$ for $p < q$. The factors of the product $a_{j_1}^{z_1} \cdots a_{j_\ell}^{z_\ell}(j_p)$ are given by s, e, f . The factor s occurs at least twice since $a_{j_p}(j_p) = a_{j_q}(j_p) = s$. By Lemma 2.2 this product does not yield s , contradicting our assumption. We define an assignment

$$\begin{aligned} \theta: x_{j_1} &\mapsto z_1, \dots, x_{j_\ell} \mapsto z_\ell, \\ x_j &\mapsto 0 \quad \text{for } j \in [k] \setminus \{j_1, \dots, j_\ell\}, \end{aligned}$$

and show that θ satisfies the formula Φ . Let $i \in [m]$. Since $a_{j_1}^{z_1} \cdots a_{j_\ell}^{z_\ell}(k+i)$ is a product in e, g that yields g , some factor $a_{j_p}^{z_p}(k+i)$ must be g . From the definition of $a_{j_p}^{z_p}$ we see that either $z_p = 0$ and $\neg x_{j_p} \in C_i$, or $z_p = 1$ and $x_{j_p} \in C_i$. This means the formula $\bigvee C_i$ is satisfied under the assignment θ . Since i was arbitrary, Φ is also satisfied. The equivalence (1) and the theorem are proved. \square

Corollary 2.3. *If a \mathcal{J} -class of a finite semigroup S contains both group and non-group \mathcal{H} -classes, then $\text{SMP}(S)$ is NP-hard.*

Proof. Let $s \in S$ such that H_s is not a group and J_s contains group \mathcal{H} -classes. From Green's Theorem [3, Theorem 2.2.5] we know that s does not generate a group. Since J_s contains an idempotent and $J_s = D_s$, the element s is regular by [3, Proposition 2.3.1]. That is, there is a $u \in S$ such that $sus = s$. Now su, s , and us fulfill the hypothesis of Theorem 1.1. \square

3. COMBINATORIAL REES MATRIX SEMIGROUPS

In this section we will establish a P/NP-complete dichotomy for the SMP for combinatorial Rees matrix semigroups by proving Theorem 1.2. After that we apply this result to combinatorial 0-simple semigroups.

Combinatorial Rees matrix semigroups have the following property:

Lemma 3.1 (cf. [9, Lemma 2.2]). *Let $k \geq 2$ and a_1, \dots, a_k be elements of a combinatorial Rees matrix semigroup S_P .*

- (a) *We have $a_1 \cdots a_k = 0$ if and only if $a_j a_{j+1} = 0$ for some $j \in [k-1]$.*
- (b) *If $a_1 \cdots a_k \neq 0$, then there are $i, j \in I$ and $\lambda, \mu \in \Lambda$ such that $a_1 = [i, \lambda]$, $a_k = [j, \mu]$, and $a_1 \cdots a_k = [i, \mu]$.*

Proof. Straightforward. \square

The next two results will allow us to show that the SMP for a combinatorial Rees matrix semigroup is in NP.

Lemma 3.2 (cf. [9, Theorem 4.3]). *Let $f := y_1 \cdots y_k$ and $g := z_1 \cdots z_\ell$ be words over an alphabet X such that*

- (a) $\{y_i y_{i+1} \mid i \in [k-1]\} = \{z_j z_{j+1} \mid j \in [\ell-1]\}$,
- (b) $y_1 = z_1$ and $y_k = z_\ell$.

Then every combinatorial Rees matrix semigroup S_P satisfies $f \approx g$.

Proof. Let S_P be a combinatorial Rees matrix semigroup, and let $\alpha: X^+ \rightarrow S_P$ be a homomorphism from the free semigroup over X to S_P . By item (a) we have $\{y_1, \dots, y_k\} = \{z_1, \dots, z_\ell\}$. We claim that

$$(3) \quad \alpha(y_1 \cdots y_k) = 0 \quad \text{if and only if} \quad \alpha(z_1 \cdots z_\ell) = 0.$$

Assume $\alpha(y_1 \cdots y_k) = 0$. Then $\alpha(y_i)\alpha(y_{i+1}) = 0$ for some $i \in [k-1]$ by Lemma 3.1 (a). By item (a) $y_i y_{i+1} = z_j z_{j+1}$ for some $j \in [\ell-1]$. Thus $\alpha(z_j)\alpha(z_{j+1}) = 0$, and hence $\alpha(z_1 \cdots z_\ell) = 0$. This proves (3).

If $\alpha(y_1 \cdots y_k) = 0$, then $\alpha(y_1 \cdots y_k) = \alpha(z_1 \cdots z_\ell)$ by (3). Assume $\alpha(y_1 \cdots y_k) \neq 0$. Then also $\alpha(z_1 \cdots z_\ell) \neq 0$, and Lemma 3.1 (b) implies

$$\alpha(y_1) \cdots \alpha(y_k) = \alpha(z_1) \cdots \alpha(z_\ell).$$

This proves the lemma. \square

Lemma 3.3. *Let f be a word over x_1, \dots, x_k . Then there is a word g such that*

- (a) *the length of g is at most $k(k^2 + 1)$, and*
- (b) *every combinatorial Rees matrix semigroup satisfies $f \approx g$.*

Proof. Let $f = y_1 \cdots y_\ell$ for $y_1, \dots, y_\ell \in \{x_1, \dots, x_k\}$. We show that there is a word g such that item (b) holds and in which each variable x_i occurs at most $k^2 + 1$ times. Fix $i \in [k]$. Let $j_1, \dots, j_m \in [\ell]$ be the positions of x_i in $y_1 \cdots y_\ell$. Let

$$\begin{aligned} v_1 &:= y_1 \cdots y_{j_1}, \\ v_r &:= y_{j_{r-1}+1} \cdots y_{j_r} \quad \text{for } r \in \{2, \dots, m\}, \\ v_{m+1} &:= y_{j_m+1} \cdots y_\ell. \end{aligned}$$

Note that $f = v_1 \cdots v_{m+1}$. Now for every word $h := z_1 \cdots z_n$ over x_1, \dots, x_k let

$$E(h) := \{z_j z_{j+1} \mid j \in [n-1]\}.$$

It is not hard to see that

$$E(v_1 \cdots v_r) = E(v_1) \cup E(x_i v_2) \cup \dots \cup E(x_i v_r) \quad \text{for } r \in \{2, \dots, m+1\}.$$

We define

$$R := \{r \in \{2, \dots, m\} \mid E(x_i v_r) \not\subseteq E(v_1 \cdots v_{r-1})\}$$

and let

$$g := v_1 \left(\prod_{r \in R} v_r \right) v_{m+1}.$$

Apparently g is a concatenation of subwords of f , and f and g start with the same letter. We show that

$$(4) \quad f \text{ and } g \text{ also end with the same letter.}$$

If v_{m+1} is nonempty, then (4) is clear. If v_{m+1} is empty, then $y_\ell = x_i$, and g ends with a subword v_r for some $r \in [m]$. Since v_r and f both end with x_i , (4) is proved. We have

$$\begin{aligned} E(f) &= E(v_1 \cdots v_{m+1}) = E(v_1) \cup \bigcup_{r=2}^m E(x_i v_r) \cup E(x_i v_{m+1}) \\ &= E(v_1) \cup \bigcup_{r \in R} E(x_i v_r) \cup E(x_i v_{m+1}) = E(g). \end{aligned}$$

Now Lemma 3.2 implies item (b).

Next observe that $|R| \leq k^2$ by the definitions of R and E . This means x_i occurs at most $k^2 + 1$ times in g . Since x_i was arbitrary, we can reduce the number of occurrences of each variable in f to at most $k^2 + 1$. Item (a) is proved. \square

Lemma 3.4. *The SMP for a finite combinatorial Rees matrix semigroup is in NP.*

Proof. Let S be such a semigroup, and let $\{a_1, \dots, a_k\} \subseteq S^n$, $b \in S^n$ be an instance of $\text{SMP}(S)$. If $b \in \langle a_1, \dots, a_k \rangle$, then there is a term function f such that $f(a_1, \dots, a_k) = b$. By Lemma 3.3 there is a word g which induces f and whose length is polynomial in k . Now g witnesses the positive answer. \square

For the following result note that the all-0 matrix has one block.

Lemma 3.5. *Let S_P be a finite combinatorial Rees matrix semigroup such that $P \in \{0, 1\}^{\Lambda \times I}$ has one block. Then Algorithm 1 decides $\text{SMP}(S_P)$ in polynomial time.*

Algorithm 1 Decides $\text{SMP}(S_P)$ in polynomial time if P has one block.

Input: $A \subseteq S_P^n$, $b \in S_P^n$,
 $m \in \{0, \dots, n\}$ such that $b(i) \neq 0$ iff $i \in [m]$,
 $J \subseteq I$, $\Delta \subseteq \Lambda$ such that $P(\lambda, i) = 1$ iff $(\lambda, i) \in \Delta \times J$ for $i \in I$, $\lambda \in \Lambda$.
Output: true if $b \in \langle A \rangle$, false otherwise.
1: **if** $b \in A$ **then**
2: **return** true
3: **end if**
4: $d := \prod \{a \in A \mid a([m]) \subseteq J \times \Delta\}$ (some order)
5: **return** $\exists a_1, a_2 \in A: a_1 d a_2 = b$

Proof. Fix an input $A \subseteq S_P^n$, $b \in S_P^n$. We may assume that there is an $m \in \{0, \dots, n\}$ such that

$$\begin{aligned} b(i) &\neq 0 && \text{for } i \in [m], \\ b(i) &= 0 && \text{for } i \in \{m+1, \dots, n\}. \end{aligned}$$

Correctness of Algorithm 1. If Algorithm 1 returns true, then clearly $b \in \langle A \rangle$. Conversely assume $b \in \langle A \rangle$. We show that true is returned. Let $g_1, \dots, g_k \in A$ such that $b = g_1 \cdots g_k$. If $k = 1$ then true is returned in line 2. Assume $k \geq 2$. We have

$$(5) \quad \begin{aligned} g_1(i) &\in I \times \Delta, \quad g_k(i) \in J \times \Lambda, \quad \text{and} \\ g_2(i), \dots, g_{k-1}(i) &\in J \times \Delta \quad \text{for all } i \in [m]; \end{aligned}$$

otherwise we obtain the contradiction $g_1 \cdots g_k(i) = 0$ for some $i \in [m]$. Let d have a value assigned by line 4. We claim that

$$(6) \quad g_1 d g_k = b.$$

For $i \in [m]$ we have $d(i) \in J \times \Delta$. The multiplication rule and (5) imply

$$b(i) = g_1 \cdots g_k(i) = g_1 d g_k(i).$$

Now let $i \in \{m+1, \dots, n\}$. Since $b(i) = 0$, there are three cases: $g_1(i) \notin I \times \Delta$, $g_k(i) \notin J \times \Lambda$, or $g_j(i) \notin J \times \Delta$ for some $j \in \{2, \dots, k-1\}$. In the first two cases $g_1 d g_k(i) = 0 = b(i)$ holds. In the third case $a := g_j$ occurs as factor in line 4. Thus

$d(i) \notin J \times \Delta$, and hence $g_1 dg_k(i) = 0$. This proves (6). So the algorithm returns true in line 5.

Complexity of Algorithm 1. The product in line 4 can be computed in $\mathcal{O}(|A|n)$ time. Checking the condition in line 5 requires $\mathcal{O}(|A|^2n)$ time. Altogether Algorithm 1 runs in $\mathcal{O}(|A|^2n)$ time. \square

Now we prove Theorem 1.2 and Corollary 1.3.

Proof of Theorem 1.2. Assume $P \in \{0, 1\}^{\Lambda \times I}$. If P has one block, then $\text{SMP}(S_P)$ is in P by Lemma 3.5. Assume P does not have one block. Then there are $i, j \in I$ and $\lambda, \mu \in \Lambda$ such that

$$P(\lambda, i) = P(\mu, j) = 1 \quad \text{and} \quad P(\mu, i) = 0.$$

Let $r := [i, \lambda]$, $s := [i, \mu]$, and $t := [j, \mu]$. Then $rs = st = s$, and s does not generate a group. By Theorem 1.1 $\text{SMP}(S_P)$ is NP-hard. NP-easiness follows from Lemma 3.4. \square

Proof of Corollary 1.3. The result is immediate from Theorem 1.2. \square

Next we restate the Rees Theorem (see [3, Theorem 3.2.3]) for the case of finite combinatorial 0-simple semigroups:

Theorem 3.6 (Rees Theorem). *Let P be a finite 0-1 matrix such that each row and each column has at least one 1. Then S_P is a finite combinatorial 0-simple semigroup.*

Conversely, every finite combinatorial 0-simple semigroup is isomorphic to one constructed in this way.

Proof. See [3]. \square

Lemma 3.7. *Let S_P be a finite combinatorial 0-simple semigroup. Then the matrix P has one block if and only if S_P has no zero divisors, i.e. for $s, t \in S_P$, $st = 0$ implies that $s = 0$ or $t = 0$.*

Proof. Assume $P \in \{0, 1\}^{\Lambda \times I}$. If P has one block, then all entries of P are 1. Thus S_P has no zero divisors. If P does not have one block, then $P(\lambda, i) = 0$ for some $\lambda \in \Lambda$, $i \in I$. Now $[i, \lambda]$ is a zero divisor since $[i, \lambda]^2 = 0$. \square

Corollary 3.8. *If a finite combinatorial 0-simple semigroup S has no zero divisors, then $\text{SMP}(S)$ is in P. Otherwise $\text{SMP}(S)$ is NP-complete.*

Proof. The result is immediate from Theorem 1.2 and Lemma 3.7. \square

4. SEMIGROUPS WITH PSPACE-COMPLETE SMP

In [1] an upper bound on the complexity of the SMP for semigroups was established:

Theorem 4.1 ([1, Theorem 2.1]). *The SMP for a finite semigroup is in PSPACE.*

Proof. Let S be a finite semigroup. We show that

$$(7) \quad \text{SMP}(S) \text{ is in nondeterministic linear space.}$$

To this end, let $A \subseteq S^n$, $b \in S^n$ be an instance of $\text{SMP}(S)$. If $b \in \langle A \rangle$, then there exist $a_1, \dots, a_m \in A$ such that $b = a_1 \cdots a_m$.

Now we pick the first generator $a_1 \in A$ nondeterministically and start with $c := a_1$. Pick the next generator $a \in A$ nondeterministically, compute $c := c \cdot a$, and repeat until we obtain $c = b$. Clearly all computations can be done in space linear in $|A|n$. This proves (7). By a result of Savitch [8] this implies that $\text{SMP}(S)$ is in deterministic quadratic space. \square

In [1] it was shown that the SMP for the full transformation semigroup on 5 letters is PSPACE-complete by reducing Q3SAT to $\text{SMP}(T_5)$. We adapt the proof of this result and show that under the following conditions the SMP for a semigroup is PSPACE-complete.

Lemma 4.2. *Let S be a finite semigroup and $s, t, \underline{1} \in S$ such that*

- (a) $sts = s, tst = t$,
- (b) $s^2, t^2 <_{\mathcal{J}} s$,
- (c) $s\underline{1} = s$ and $t\underline{1} = t$.

Then $\text{SMP}(S)$ is PSPACE-complete.

Proof. From item (a) we know that s, t, st, ts are in the same \mathcal{J} -class. Observe that $s \neq st$; otherwise $s^2 = sts = s$, which is impossible. We consider s and st as states and let $\underline{1}, s, t, st, ts$ act on these states by multiplication on the right. This yields the partial multiplication table

$$(8) \quad \begin{array}{c|ccccc} S & \underline{1} & s & t & st & ts \\ \hline s & s & \infty & st & \infty & s \\ st & st & s & \infty & st & \infty \end{array}$$

where ∞ means that this entry is $<_{\mathcal{J}} s$.

$\text{SMP}(S)$ is in PSPACE by Theorem 4.1. For PSPACE-hardness we reduce Q3SAT to $\text{SMP}(S)$. Q3SAT is PSPACE-complete [7] and can be defined as follows.

Q3SAT

Input: triples C_1, \dots, C_m over $\{x_1, \dots, x_n, \neg x_1, \dots, \neg x_n, y_1, \dots, y_n, \neg y_1, \dots, \neg y_n\}$

Problem: Is the Boolean formula $\Phi := \forall x_1 \exists y_1 \dots \forall x_n \exists y_n (\bigvee C_1) \wedge \dots \wedge (\bigvee C_m)$ true?

Let C_1, \dots, C_m be a Q3SAT instance and Φ be the corresponding Boolean formula. We refer to x_1, \dots, x_n as *universal variables*, to y_1, \dots, y_n as *existential variables*, and to C_1, \dots, C_m as *clauses*.

We define the corresponding $\text{SMP}(S)$ instance

$$G \subseteq S^{3n+m+1}, f \in S^{3n+m+1}$$

where

$$\begin{aligned} G &:= \{a\} \cup B \cup C \cup D \cup E, \\ B &:= \{b_1, \dots, b_n\}, \\ C &:= \{c_j^k \mid j \in [m], k \in \{+, -, 0\}\}, \\ D &:= \{d_{jk} \mid j \in [m], k \in [3]\}, \\ E &:= \{e_1, \dots, e_n\}. \end{aligned}$$

The coordinates of these tuples will have the following meaning. The first n positions encode truth values assigned to x_1, \dots, x_n , and the second n positions truth values assigned to y_1, \dots, y_n . Truth values are represented by

$$0 := s \quad \text{and} \quad 1 := st.$$

The positions $2n + 1$ to $3n$ control the order in which the given tuples are multiplied. The m positions after that indicate the status of the clauses C_1, \dots, C_m . In particular, for $i \in [m]$ position $3n + i$ encodes whether $\bigvee C_i$ is satisfied by the assignment given by the first $2n$ positions. We encode

“unsatisfied” by s , and “satisfied” by st .

The last position ensures that the first generator of the target tuple f is the tuple a . The generators are explicitly given as follows. For an overview see Figure 1.

- We define our target tuple f by

$$\begin{aligned} f(i) &:= st \quad \text{for } i \in [3n + m], \\ f(3n + m + 1) &:= s. \end{aligned}$$

- The tuple a will be the first generator of f . It encodes the all-zero assignment for the variables $x_1, \dots, x_n, y_1, \dots, y_n$. Let

$$a(i) := s \quad \text{for } i \in [3n + m + 1].$$

The idea is that a is multiplied only on the right by elements of G . The components of this product are the states s and st . Each multiplication on the right modifies the states according to the multiplication table (8).

- For $j \in [n]$ let b_j change the assignment for the universal variables

$$\text{from } (x_1, \dots, x_{j-1}, 0, 1, \dots, 1) \text{ to } (x_1, \dots, x_{j-1}, 1, 0, \dots, 0).$$

For $j \in [n]$ define

$$\begin{aligned} b_j(i) &:= \begin{cases} \underline{1} & \text{if } i \in [j - 1] \text{ or } n + 1 \leq i \leq 2n, \\ t & \text{if } i = j, \\ s & \text{if } j < i \leq n, \end{cases} \\ b_j(2n + i) &:= \begin{cases} st & \text{if } i \in [j - 1], \\ s & \text{if } j \leq i \leq m + n, \end{cases} \\ b_j(3n + m + 1) &:= ts. \end{aligned}$$

- For $j \in [n]$ let c_j^+ and c_j^- change the assignment for the existential variable y_j from 0 to 1 and from 1 to 0, respectively. Let c_j^0 leave the variables unchanged. For $j \in [n]$ and $i \in [3n + m + 1]$ let

$$c_j^0(i) := \begin{cases} t & \text{if } i = 2n + j, \\ st & \text{if } i = 3n + m + 1, \\ \underline{1} & \text{otherwise.} \end{cases}$$

The tuples c_j^+ and c_j^- differ from c_j^0 only in the following positions:

$$c_j^+(n + j) := t, \quad c_j^-(n + j) := s.$$

- For $j \in [m]$ and $k \in [3]$ the tuple d_{jk} evaluates the k th literal C_{jk} of the j th clause. If this literal is satisfied by the assignment encoded in the first $2n$ components, then multiplying by d_{jk} changes the status of the clause C_j to “satisfied”. This will be more formally stated in Claim 4.3. For $i \in [n]$ define

$$\begin{aligned} d_{jk}(i) &:= \begin{cases} st & \text{if } C_{jk} = x_i, \\ ts & \text{if } C_{jk} = \neg x_i, \\ \underline{1} & \text{otherwise,} \end{cases} \\ d_{jk}(n+i) &:= \begin{cases} st & \text{if } C_{jk} = y_i, \\ ts & \text{if } C_{jk} = \neg y_i, \\ \underline{1} & \text{otherwise,} \end{cases} \\ d_{jk}(2n+i) &:= st. \end{aligned}$$

For $i \in [m]$ let

$$\begin{aligned} d_{jk}(3n+i) &:= \begin{cases} t & \text{if } i = j, \\ \underline{1} & \text{otherwise,} \end{cases} \\ d_{jk}(3n+m+1) &:= ts. \end{aligned}$$

- Let $j \in [n]$. After each assignment was successfully evaluated, the tuple e_j sets position $n+j$ to st in order to match the target tuple if necessary. We define

$$\begin{aligned} e_j(i) &:= st, \quad \text{for } i \in [n], \\ e_j(n+i) &:= \begin{cases} t & \text{if } i = j, \\ \underline{1} & \text{if } i \in [2n] \setminus \{j\}, \end{cases} \\ e_j(3n+i) &:= st \quad \text{for } i \in [m], \\ e_j(3n+m+1) &:= ts. \end{aligned}$$

The tuples e_1, \dots, e_n will only occur as final generators of f .

Now we state what we already mentioned in the definition of d_{jk} .

Claim 4.3. *Let $h \in \langle G \rangle$ such that*

$$\begin{aligned} h(i) &\in \{s, st\} \quad \text{for all } i \in [2n], \\ h(2n+i) &= st \quad \text{for all } i \in [n], \\ h(3n+j) &= s \quad \text{for some } j \in [m], \\ h(3n+m+1) &= s. \end{aligned}$$

Let $\rho: \{x_1, \dots, x_n, y_1, \dots, y_n\} \rightarrow \{0, 1\}$ be the assignment encoded by $h|_{[2n]}$, i.e.

$$\begin{aligned} \rho(x_i) &:= h(i) \quad \text{for } i \in [n], \\ \rho(y_i) &:= h(n+i) \quad \text{for } i \in [n]. \end{aligned}$$

Let $k \in [3]$, C_{jk} be the k th literal of the j th clause, and $h' := hd_{jk}$.

- (a) If $\rho(C_{jk}) = 1$, then h and h' differ only in the following position:

$$h'(3n+j) = st.$$

- (b) Otherwise $h'(i) <_{\mathcal{J}} s$ for some $i \in [2n]$.

$$\begin{aligned}
a &= (s \ \cdots \ s \ s \ \cdots \ s \ s \ \cdots \ s \ s \ \cdots \ s \ s) \\
b_1 &= (t \ s \ s \ \quad \quad \quad s \ \cdots \ s \ s \ \cdots \ s \ ts) \\
\vdots &= (\quad \quad \quad \ddots \ s \ \quad \quad \quad st \ \ddots \ \vdots \ \vdots \ \ddots \ \vdots \ \vdots) \\
b_n &= (\quad \quad \quad t \ \quad \quad \quad st \ st \ s \ s \ \cdots \ s \ ts) \\
c_1^+ &= (\quad \quad \quad t \ \quad \quad \quad t \ \quad \quad \quad ts) \\
\vdots &= (\quad \quad \quad \ddots \ \quad \quad \quad \ddots \ \quad \quad \quad \vdots) \\
c_n^+ &= (\quad \quad \quad t \ \quad \quad \quad t \ \quad \quad \quad ts) \\
c_1^- &= (\quad \quad \quad s \ \quad \quad \quad t \ \quad \quad \quad ts) \\
\vdots &= (\quad \quad \quad \ddots \ \quad \quad \quad \ddots \ \quad \quad \quad \vdots) \\
c_n^- &= (\quad \quad \quad s \ \quad \quad \quad t \ \quad \quad \quad ts) \\
c_1^0 &= (\quad \quad \quad t \ \quad \quad \quad ts) \\
\vdots &= (\quad \quad \quad \ddots \ \quad \quad \quad \vdots) \\
c_n^0 &= (\quad \quad \quad t \ \quad \quad \quad ts) \\
d_{1k} &= (* \ \cdots \ * \ * \ \cdots \ * \ st \ \cdots \ st \ t \ \quad \quad \quad ts) \\
\vdots &= (\vdots \ \ddots \ \vdots \ \vdots \ \ddots \ \vdots \ \vdots \ \ddots \ \vdots \ \quad \quad \quad \ddots \ \vdots) \\
d_{mk} &= (* \ \cdots \ * \ * \ \cdots \ * \ st \ \cdots \ st \ \quad \quad \quad t \ ts) \\
e_1 &= (st \ \cdots \ st \ t \ \quad \quad \quad st \ \cdots \ st \ ts) \\
\vdots &= (\vdots \ \ddots \ \vdots \ \quad \quad \quad \ddots \ \quad \quad \quad \vdots \ \ddots \ \vdots \ \vdots) \\
e_n &= (st \ \cdots \ st \ \quad \quad \quad t \ \quad \quad \quad st \ \cdots \ st \ ts) \\
f &= (\underbrace{st \ \cdots \ st}_n \ \underbrace{st \ \cdots \ st}_n \ \underbrace{st \ \cdots \ st}_n \ \underbrace{st \ \cdots \ st \ s}_m)
\end{aligned}$$

FIGURE 1. Generators and target tuple of the $\text{SMP}(T)$ instance for $k \in [3]$. Empty positions encode the element $\underline{1}$, and the symbol “*” indicates that this entry depends on the Q3SAT instance.

Proof. The literal C_{jk} is of the form z or $\neg z$ for some variable z . Let $\ell \in [2n]$ be the position of z in $(x_1, \dots, x_n, y_1, \dots, y_n)$. First assume C_{jk} is of the form z . Then $d_{jk}(\ell) = st$.

(a) Assume $\rho(C_{jk}) = 1$. This means $h(\ell) = st$. Thus $h'(\ell) = st \cdot st = st = h(\ell)$, and $h'(3n+j) = s \cdot t = st$. It is easy to see that $h(i) = h'(i)$ for the remaining positions $i \in [3n+m+1] \setminus \{\ell, 3n+j\}$.

(b) Assume $\rho(C_{jk}) = 0$. This means $h(\ell) = s$. Thus $h'(\ell) = s \cdot st <_{\mathcal{J}} s$, and (b) is proved.

If C_{jk} is of the form $\neg z$, then (a) and (b) are proved in a similar way. \square

Note that if ρ satisfies C_{jk} , then multiplying h by d_{jk} changes the status of the j th clause from “unsatisfied” to “satisfied”. Otherwise the target tuple f cannot be reached by further multiplying hd_{jk} with elements of G .

In the remainder of the proof we show the following.

Claim 4.4. Φ holds if and only if $f \in \langle G \rangle$.

(\Rightarrow) *direction of Claim 4.4.* Assume Φ is true. This means that for every $i \in [n]$ there is a function $\psi_i : \{0, 1\}^i \rightarrow \{0, 1\}$ such that for every assignment $\varphi : \{x_1, \dots, x_n\} \rightarrow \{0, 1\}$ the assignment

$$\rho_\varphi := \varphi \cup \{y_i \mapsto \psi_i(\varphi(x_1), \dots, \varphi(x_i)) \mid i \in [n]\}$$

satisfies all the clauses C_1, \dots, C_m .

We prove by induction on assignments φ in lexicographic order that for each φ the following tuple g_φ belongs to $\langle G \rangle$:

$$\begin{aligned} g_\varphi(i) &:= \varphi(x_i) && \text{for } i \in [n], \\ g_\varphi(n+i) &:= \rho_\varphi(y_i) && \text{for } i \in [n], \\ g_\varphi(2n+i) &:= st && \text{for } i \in [n+m], \\ g_\varphi(3n+m+1) &:= s. \end{aligned}$$

For the base case let $\varphi(x_i) := 0$ for all $i \in [n]$. For $i \in [n]$ we define

$$c'_i := \begin{cases} c_i^+ & \text{if } \rho_\varphi(y_i) = 1, \\ c_i^0 & \text{otherwise.} \end{cases}$$

Apparently $a \cdot c'_1 \cdots c'_n$ encodes ρ_φ . For each $j \in [m]$ there is a $k_j \in [3]$ such that the literal C_{jk_j} is satisfied by ρ_φ . By Claim 4.3 (a) it is straightforward to verify that

$$g_\varphi = a \cdot c'_1 \cdots c'_n \cdot d_{1k_1} \cdots d_{mk_m}.$$

Now let φ be an assignment with successor φ' in lexicographical order such that $g_\varphi \in \langle G \rangle$. Let $j \in [n]$ be maximal such that $\varphi(x_j) = 0$. Then

$$\begin{aligned} \varphi(x_i) &= \varphi'(x_i) && \text{for } i < j, \\ \varphi(x_j) &= 0, \varphi'(x_j) = 1, \\ \varphi(x_i) &= 1, \varphi'(x_i) = 0 && \text{for } j < i \leq n. \end{aligned}$$

To adjust the assignment for the existential variables, for $j \leq i \leq n$ set

$$c'_i := \begin{cases} c_i^+ & \text{if } \rho_\varphi(y_i) = 0, \rho_{\varphi'}(y_i) = 1, \\ c_i^- & \text{if } \rho_\varphi(y_i) = 1, \rho_{\varphi'}(y_i) = 0, \\ c_i^0 & \text{otherwise.} \end{cases}$$

For $h := g_\varphi \cdot b_j \cdot c'_j \cdots c'_n$ we have

$$\begin{aligned} h(i) &= \varphi'(x_i) && \text{for } i \in [n], \\ h(n+i) &= \rho_{\varphi'}(y_i) && \text{for } i \in [n], \\ h(2n+i) &= st && \text{for } i \in [n], \\ h(3n+i) &= s && \text{for } i \in [m+1]. \end{aligned}$$

For each $j \in [m]$ the clause C_j is satisfied by $\rho_{\varphi'}$. Thus there is a $k_j \in [3]$ such that $\rho_{\varphi'}$ satisfies the literal C_{jk_j} . From Claim 4.3 (a) follows that

$$g_{\varphi'} = h \cdot d_{1k_1} \cdots d_{mk_m}.$$

This completes the induction argument.

Finally let φ be such that $\varphi(x_i) = 1$ for all $i \in [n]$, and g_φ as defined above. Denote the positions $i \in [n]$ where $g_\varphi(n+i) = s$ by i_1, \dots, i_p . Then we have

$$f = g_\varphi \cdot e_{i_1} \cdots e_{i_p}.$$

Thus $f \in \langle G \rangle$. The (\Rightarrow) direction of Claim 4.4 is proved.

We give another description of the product that yields f . For each assignment $\varphi \neq 0$ for x_1, \dots, x_n let $j_\varphi := \max\{j \in [n] \mid \varphi(x_j) = 1\}$. From our argument above we see that f is of the form

$$(9) \quad f = ac_1^* \cdots c_n^* d_{1\dagger} \cdots d_{m\dagger} \cdot \left(\prod_{\varphi \neq 0} b_{j_\varphi} c_{j_\varphi}^* \cdots c_n^* d_{1\dagger} \cdots d_{m\dagger} \right) \cdot e_{i_1} \cdots e_{i_p},$$

where $i_1, \dots, i_p \in [n]$ are distinct, each $*$ belongs to $\{+, -, 0\}$, and each \dagger to $[3]$. The product is taken over all assignments $\varphi \neq 0$ to x_1, \dots, x_n in lexicographical order.

(\Leftarrow) *direction of Claim 4.4.* Assume $f \in \langle G \rangle$. Let $k \in \mathbb{N}$ be minimal such that $f = u_1 \cdots u_k$ for some $u_1, \dots, u_k \in G$, and let $v_i := u_1 \cdots u_i$ for $i \in [k]$.

Claim 4.5. *Let $i \in \{2, \dots, k\}$ and $j \in [3n + m + 1]$. Then*

- (a) $u_1 = a$ and $u_i \neq a$,
- (b) $v_i(j) \in \{s, st\}$.
- (c) *If $u_i(j) \in \{\underline{1}, st, ts\}$, then $v_i(j) = v_{i-1}(j)$.*

Proof. (a) If $u_i = a$, then $u_{i-1}u_i(3n + m + 1) \in \{ts^2, s^2\}$, which yields the contradiction $v_k(3n + m + 1) <_{\mathcal{J}} s$. If $u_1 \neq a$, then we obtain the contradiction $v_k(3n + m + 1) = ts$.

(b) We use induction on i . By (a) we have $v_1 = a$. Thus $v_1(j) \in \{s, st\}$. Now assume $v_{i-1}(j) \in \{s, st\}$. Since $u_i(j) \in \{\underline{1}, s, st, t, ts\}$, either $v_i(j) \in \{s, st\}$, or a factor s^2 or t^2 occurs in $v_i(j)$. As $s^2, t^2 <_{\mathcal{J}} f(j)$, the first case applies.

(c) is immediate from item (b) and the multiplication table (8). \square

The next claim states that the product $u_1 \cdots u_k$ is of a similar form to the one given in (9).

Claim 4.6. *Let $i \in [k]$. Let either $j \in [n]$ and $u_i = b_j$, or $j = 1$ and $u_i = a$. Then for $i_1 := i + n - j + 1$ and $i_2 := i_1 + m$ the following holds:*

- (a) $\{u_{i_1+1}, \dots, u_{i_1}\} = \{c_j^{p_j}, \dots, c_n^{p_n}\}$ for some $p_1, \dots, p_n \in \{+, -, 0\}$.
- (b) $\{u_{i_1+1}, \dots, u_{i_2}\} = \{d_{1k_1}, \dots, d_{mk_m}\}$ for some $k_1, \dots, k_m \in [3]$.
- (c) *If there is a greatest $j' \in [n]$ such that $v_i(j') = s$, then $u_{i_2+1} = b_{j'}$;*
- (d) *otherwise u_{i_2+1}, \dots, u_k are distinct and form the set $\{e_\ell \mid \ell \in [n], v_{i_2}(n + \ell) = s\}$.*

Proof. First let $j \in [n]$ and $u_i = b_j$.

(a) From Claim 4.5 we know that $i \geq 2$ and that every coordinate of v_{i-1} is either s or st . From the definition of b_j and the multiplication table (8) we know that

$$v_i(2n + \ell) = \begin{cases} st & \text{for } \ell \in [j - 1], \\ s & \text{for } \ell \in \{j, \dots, n\}. \end{cases}$$

Thus the only choice for the $n - j + 1$ generators subsequent to u_i is given by $c_j^{p_j}, \dots, c_n^{p_n}$ for some $p_j, \dots, p_n \in \{+, -, 0\}$, where the order does not matter; otherwise we would obtain a factor s^2 or t^2 in a position $2n + \ell$ for some $\ell \in [n + m]$, which is impossible.

(b) From (a) we know that

$$\begin{aligned} v_{i_1}(2n + \ell) &= st \quad \text{for } \ell \in [n], \\ v_{i_1}(3n + \ell) &= s \quad \text{for } \ell \in [m]. \end{aligned}$$

Thus the m generators subsequent to u_{i_1} are given by $d_{1k_1}, \dots, d_{mk_m}$ for some $k_1, \dots, k_m \in [3]$ where the order does not matter; otherwise we would obtain a factor t^2 in $v_k(2n + \ell)$ for some $\ell \in [n]$, or s^2 in $v_k(3n + \ell)$ for some $\ell \in [m]$. Both cases contradict the fact that $v_k = f$.

(c) Let $j' \in [n]$ be maximal such that $v_i(j') = s$. From (a) and (b) we know that

$$\begin{aligned} v_{i_2}(j') &= s \quad \text{and} \\ v_{i_2}(2n + \ell) &= st \quad \text{for } \ell \in [n + m]. \end{aligned}$$

If $u_{i_2+1} \in E$, then $v_{i_2+1}(j') = s^2t$. If $u_{i_2+1} \in C \cup D$, then $v_{i_2+1}(2n + \ell) = st^2$ for some $\ell \in [n + m]$. Thus $u_{i_2+1} = b_\ell$ for some $\ell \in [n]$. If $\ell < j'$, then $v_{i_2+1}(j') = s^2$. If $\ell > j'$, then $v_{i_2+1}(\ell) = st^2$. Therefore $\ell = j'$.

(d) Assume $v_i(\ell) = st$ for all $\ell \in [n]$. Suppose some generator among u_{i_2+1}, \dots, u_k belongs to B . Let $i_3 \in \{i_2 + 1, \dots, k\}$ be minimal such that $u_{i_3} \in B$. By (a), (b), and Claim 4.5 (c) we have

$$v_i|_{[n]} = \dots = v_{i_3-1}|_{[n]}.$$

Thus $v_{i_3}(\ell) = st^2$ for some $\ell \in [n]$, which is impossible. Hence $u_{i_2+1}, \dots, u_k \notin B$. This together with (a) and (b) implies

$$v_{i_2}(2n + \ell) = \dots = v_k(2n + \ell) = st \quad \text{for all } \ell \in [n + m].$$

Thus $u_{i_2+1}, \dots, u_k \notin C \cup D$. Otherwise we would have a factor t^2 in $v_k(n + \ell)$. So $u_{i_2+1}, \dots, u_k \in E$. If u_{i_2+1}, \dots, u_k were not distinct, then we had a factor t^2 in $v_k(n + \ell)$ for some $\ell \in [n]$. Finally observe that for each $\ell \in [n]$ with $v_{i_2}(n + \ell) = s$ we have $e_\ell \in \{u_{i_2+1}, \dots, u_k\}$; otherwise $v_k(n + \ell) = s$ which is impossible. We proved (d).

For $j = 1$ and $u_i = a$, items (a) to (d) are proved in a similar manner. \square

In the following we define assignments to the variables using the first $2n$ positions of the tuples v_1, \dots, v_k . For $i \in [k]$ and $j \in [n]$ let

$$\begin{aligned} \varphi_i: \{x_1, \dots, x_n\} &\rightarrow \{0, 1\}, \quad \varphi_i(x_j) := v_i(j), \\ \theta_i: \{y_1, \dots, y_n\} &\rightarrow \{0, 1\}, \quad \theta_i(y_j) := v_i(n + j). \end{aligned}$$

These assignments fulfill the following conditions.

Claim 4.7.

- (a) For $i \in [k - 1]$ we have $\varphi_i \neq \varphi_{i+1}$ if and only if $u_{i+1} \in B$.
- (b) $\varphi_1, \dots, \varphi_k$ is a list of all assignments for x_1, \dots, x_n (possibly with repetitions) in lexicographic order.
- (c) Let $i \in [k - 1]$ such that $u_i \in D$ and $u_{i+1} \notin D$. Then $\varphi_i \cup \theta_i$ satisfies all the clauses C_1, \dots, C_m .

Proof. (a) follows from the definitions of the generators, Claim 4.5 (c), and Claim 4.6.

(b) Let $i \in [k - 1]$ such that $\varphi_i \neq \varphi_{i+1}$. By (a) and Claim 4.6 $u_{i+1} = b_j$ for the greatest $j \in [n]$ for which $\varphi_i(x_j) = 0$. It is easy to see that $\varphi_{i+1}(x_\ell) = \varphi_i(x_\ell)$ for $\ell < j$, $\varphi_{i+1}(x_j) = 1$, and $\varphi_{i+1}(x_\ell) = 0$ for $\ell > j$. Thus φ_{i+1} is the successor of φ_i in lexicographic order. By Claim 4.5 (a) φ_1 is the all-zero assignment for x_1, \dots, x_n .

Since $v_k(i) = st$ for all $i \in [n]$, φ_k is the all-one assignment. Hence $\varphi_1, \dots, \varphi_k$ is a list of all assignments.

(c) By Claim 4.6 $\{u_{i-m+1}, \dots, u_i\} = \{d_{1k_1}, \dots, d_{mk_m}\}$ for some $k_1, \dots, k_m \in [3]$. Thus $\varphi_{i-m} \cup \theta_{i-m} = \dots = \varphi_i \cup \theta_i$. Suppose $\varphi_i \cup \theta_i$ does not satisfy some clause C_j for $j \in [m]$. Then its k th literal C_{jk_j} is also unsatisfied. Claim 4.3 (b) implies $v_i(\ell) <_{\mathcal{J}} s$ for some $\ell \in [2n]$, which is impossible. \square

For $\varphi: \{x_1, \dots, x_n\} \rightarrow \{0, 1\}$ let

$$i_\varphi := \max\{i \in [k] \mid \varphi_i = \varphi, u_i \in D\}.$$

From Claim 4.7 we know that for every assignment φ to x_1, \dots, x_n the assignment $\varphi \cup \theta_{i_\varphi}$ satisfies all the clauses of Φ . It only remains to prove that $\theta_{i_\varphi}(y_i)$ only depends on $\varphi(x_1), \dots, \varphi(x_i)$.

Claim 4.8. *Let $i \in [n]$. For all $\varphi, \chi: \{x_1, \dots, x_n\} \rightarrow \{0, 1\}$ the equations*

$$(10) \quad \varphi(x_1) = \chi(x_1), \dots, \varphi(x_i) = \chi(x_i)$$

imply $\theta_{i_\varphi}(y_i) = \theta_{i_\chi}(y_i)$.

Proof. We consider φ as fixed and prove the implication for all $\chi \geq \varphi$ by induction in lexicographical order. The base case $\chi = \varphi$ is clear.

Now let $\chi \geq \varphi$ be an assignment for which the implication holds, and assume its successor χ' fulfills (10). Since $\varphi \leq \chi < \chi'$, the assignment χ also fulfills (10). From Claim 4.6 we know that

$$(11) \quad \{u_{i_\chi+1}, \dots, u_{i_{\chi'}}\} = \{b_j, c_j^{p_j}, \dots, c_n^{p_n}, d_{1k_1}, \dots, d_{mk_m}\}$$

for some $j \in [n]$, $p_j, \dots, p_n \in \{+, -, 0\}$, and $k_1, \dots, k_m \in [3]$. If $j \leq i$ was true, then χ' would not fulfill (10). Thus $j > i$. From (11) follows $v_{i_{\chi'}}(n+i) = v_{i_\chi}(n+i)$. Thus $\theta_{i_{\chi'}}(y_i) = \theta_{i_\chi}(y_i) = \theta_{i_\varphi}(y_i)$, and Claim 4.8 is proved. \square

We complete the proof of Claim 4.4. By Claims 4.7 and 4.8, for each assignment φ for the universal variables there is an assignment θ_{i_φ} for the existential variables such that $\varphi \cup \theta_{i_\varphi}$ satisfies the conjunctive normal form in Φ . For all $i \in [n]$ the value $\theta_{i_\varphi}(y_i)$ depends only on $\varphi(x_1), \dots, \varphi(x_i)$. Thus Φ is true. Claim 4.4 and Lemma 4.2 are proved. \square

Proof of Theorem 1.4. Let $s' := (s, tst)$, $t' := (tst, s)$, and $\underline{1}' := (\underline{1}, \underline{1})$ be elements of $S^2 := S \times S$. Apparently $s't's' = s'$ and $t's't' = t'$. Both s' and t' do not generate groups. By Lemma 2.1 $s'^2 <_{\mathcal{J}} s'$ and $t'^2 <_{\mathcal{J}} t'$. Since $t' \mathcal{J} s'$, we have $t'^2 <_{\mathcal{J}} s'$. Now $s', t', \underline{1}'$ fulfill the hypothesis of Lemma 4.2. Thus $\text{SMP}(S^2)$ is PSPACE-complete. As $\text{SMP}(S^2)$ reduces to $\text{SMP}(S)$ and conversely, the result follows. \square

Now we are able to list several “naturally occurring” semigroups with PSPACE-complete SMP:

Corollary 4.9. *The SMP for the following semigroups is PSPACE-complete:*

- (a) *the Brandt monoid B_2^1 and the monoid A_2^1 ;*
- (b) *for $n \geq 2$ and a finite ring R with identity $1 \neq 0$, the semigroup of all $n \times n$ matrices over R ;*
- (c) *the full transformation semigroup T_n on $n \geq 3$ letters;*
- (d) *the symmetric inverse semigroup I_n on $n \geq 2$ letters.*

Proof. We apply Theorem 1.4.

- (a) For B_2^1 let $s := [1, 2]$ and $t := [2, 1]$. For A_2^1 let $s := [2, 2]$ and $t := [1, 1]$.
- (b) Define $n \times n$ matrices s, t over R by

$$s_{ij} := \begin{cases} 1 & \text{if } (i, j) = (1, 2), \\ 0 & \text{otherwise,} \end{cases} \quad t_{ij} := \begin{cases} 1 & \text{if } (i, j) = (2, 1), \\ 0 & \text{otherwise} \end{cases}$$

for $i, j \in [n]$. Let $\underline{1}$ be the identity matrix.

- (c) Let $\underline{1}$ be the identity mapping on $[n]$, and $s, t: [n] \rightarrow [n]$,

$$s(x) := \begin{cases} 2 & \text{if } x = 1, \\ 3 & \text{otherwise,} \end{cases} \quad t(x) := \begin{cases} 1 & \text{if } x = 2, \\ 3 & \text{otherwise.} \end{cases}$$

- (d) Let $\underline{1}$ be the identity mapping, $s: 1 \mapsto 2$, and $t: 2 \mapsto 1$. □

For monoids we can now generalize Corollary 2.3:

Corollary 4.10. *If a \mathcal{J} -class of a finite monoid S contains both group and non-group \mathcal{H} -classes, then $\text{SMP}(S)$ is PSPACE-complete.*

Proof. Let S be as above. Similar to the proof of Corollary 2.3, there is a $t \in S$ such that $sts = s$. Now s, t , and the identity fulfill the hypothesis of Theorem 1.4. □

5. PROOF OF THEOREM 1.6

Lemma 5.1. *If the 0-1 matrix P of a finite combinatorial Rees matrix semigroup S_P has one block, then $\text{SMP}(S_P^1)$ is in NP.*

Proof. Assume $P \in \{0, 1\}^{\Lambda \times I}$, and let $J \subseteq I$ and $\Delta \subseteq \Lambda$ such that $P(\lambda, i) = 1$ if and only if $(\lambda, i) \in \Delta \times J$ for $i \in I$, $\lambda \in \Lambda$. Let $T := S_P^1$ and $A \subseteq T^n$, $b \in T^n$ be an instance of $\text{SMP}(T)$ such that $b \in \langle A \rangle$. Let $a_1, \dots, a_k \in A$ such that $b = a_1 \cdots a_k$. If $b = (1, \dots, 1)$ or $k = 1$, then clearly $b \in A$. In this case the position of b in the list A is a witness. Assume $b \neq (1, \dots, 1)$ and $k \geq 2$.

We claim that for $i \in [n]$ with $b(i) = 0$ there are $\ell_i, r_i \in [k]$, $\ell_i < r_i$ such that

$$(12) \quad a_{\ell_i} a_{r_i}(i) = 0 \quad \text{and} \quad a_{\ell_i+1}(i) = \dots = a_{r_i-1}(i) = 1.$$

This follows from Lemma 3.1 (a). For $i \in [n]$ with $b(i) \in I \times \Lambda$ let

$$\ell_i := \min\{j \in [k] \mid a_j(i) \neq 1\}, \\ r_i := \max\{j \in [k] \mid a_j(i) \neq 1\}.$$

Now define an index set $N \subseteq [k]$ by

$$N := \{\ell_i \mid i \in [n], b(i) \neq 1\} \cup \{r_i \mid i \in [n], b(i) \neq 1\}.$$

Note that $N \neq \emptyset$; otherwise $b = (1, \dots, 1)$ which contradicts our assumption.

For $i \in [n]$ we claim that

$$(13) \quad \prod_{j \in N} a_j(i) = b(i),$$

where the indexes j of the factors are in ascending order. If $b(i) = 1$, then $a_j(i) = 1$ for all $j \in [k]$, and (13) follows. Assume $b(i) = 0$. We have $\ell_i, r_i \in N$. By (12) all factors in (13) between $a_{\ell_i}(i)$ and $a_{r_i}(i)$ are equal to 1. This and (12) imply

(13). Finally assume $b(i) \in I \times \Lambda$. For $\ell_i < j < r_i$ we have $a_j(i) \in \{1\} \cup (J \times \Delta)$; otherwise we obtain the contradiction $b(i) = 0$. Thus

$$\prod_{\substack{j \in N \\ \ell_i \leq j \leq r_i}} a_j(i) = \prod_{\ell_i \leq j \leq r_i} a_j(i).$$

Since $a_j(i) = 1$ for $j < \ell_i$ and $j > r_i$, (13) follows.

The length of the product in (13) is $|N|$ and thus at most $2n$. Thus this product is a valid witness for $b \in \langle A \rangle$, and the lemma is proved. \square

Proof of Theorem 1.6. Assume $P \in \{0, 1\}^{\Lambda \times I}$.

(a) If P is the all-1 matrix, then S_P^1 is a band (idempotent semigroup) with \mathcal{J} -classes $\{0\}$, $I \times \Lambda$, and $\{1\}$. We show that S_P^1 is a *regular band*, that is, S_P^1 satisfies the identity

$$(14) \quad xyxzx = xyzx.$$

Let $x, y, z \in S_P^1$. If one of the variables is 0 or 1, then (14) clearly holds. If $x, y, z \in I \times \Lambda$, then $xyxzx = x = xyzx$ by the definition of the multiplication. Thus S_P^1 is a regular band. By [10, Corollary 1.7] the SMP for every regular band is in P.

(b) Assume P has one block and some entries are 0. Let $i \in I$ and $\lambda \in \Lambda$ such that $P(\lambda, i) = 0$. Let $s := [i, \lambda]$ and $r := t := 1$. Since s does not generate a group, $\text{SMP}(S_P^1)$ is NP-hard by Theorem 1.1. NP-easiness follows from Lemma 5.1.

(c) In this case P does not have one block. Thus there are $i, j \in I$ and $\lambda, \mu \in \Lambda$ such that

$$P(\lambda, i) = P(\mu, j) = 1 \quad \text{and} \quad P(\lambda, j) = 0.$$

Let $s := [j, \lambda]$ and $t := [i, \mu]$. Then s does not generate a group, $sts = s$, $s1 = s$, and $t1 = t$. By Theorem 1.4 $\text{SMP}(S)$ is PSPACE-complete. \square

6. CONCLUSION

In Section 3 we established a P/NP-complete dichotomy for combinatorial Rees matrix semigroups. The next goal is to investigate the complexity for the more general case of Rees matrix semigroups. For Rees matrix semigroups without 0 a polynomial time algorithm for the SMP is known [11]. However, the following questions are open:

Problem 6.1. Is the SMP for finite Rees matrix semigroups (with 0) in NP? In particular, is there a P/NP-complete dichotomy?

In Section 4 we saw the first example of a semigroup with NP-complete SMP where adjoining an identity results in a PSPACE-complete SMP. This leads to the following question:

Problem 6.2. How hard is the SMP for finite Rees matrix semigroups with adjoined identity?

The answer is not even known for the completely regular case. E.g. the complexity for the following 9-element semigroup is open:

Problem 6.3. Let $1, c$ be the elements of the cyclic group \mathbb{Z}_2 such that $c^2 = 1$, and define a Rees matrix semigroup $S := \mathcal{M}(\mathbb{Z}_2, [2], [2], \begin{pmatrix} 1 & 1 \\ 1 & c \end{pmatrix})$. How hard is $\text{SMP}(S^1)$?

REFERENCES

- [1] A. Bulatov, P. Mayr, and M. Steindl. The subpower membership problem for semigroups, submitted. Available at <http://arxiv.org/pdf/1603.09333v1.pdf>.
- [2] S. A. Cook. Characterizations of pushdown machines in terms of time-bounded computers. *J. Assoc. Comput. Mach.*, 18:4–18, 1971.
- [3] J. M. Howie. *Fundamentals of semigroup theory*, volume 12 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, New York, 1995. Oxford Science Publications.
- [4] P. Idziak, P. Marković, R. McKenzie, M. Valeriote, and R. Willard. Tractability and learnability arising from algebras with few subpowers. *SIAM J. Comput.*, 39(7):3023–3037, 2010.
- [5] M. Kozik. A finite set of functions with an EXPTIME-complete composition problem. *Theoretical Computer Science*, 407(1–3):330–341, 2008.
- [6] P. Mayr. The subpower membership problem for Mal’cev algebras. *Internat. J. Algebra Comput.*, 22(7):1250075, 23, 2012.
- [7] C. H. Papadimitriou. *Computational complexity*. Addison-Wesley Publishing Company, Reading, MA, 1994.
- [8] W. J. Savitch. Relationships between nondeterministic and deterministic tape complexities. *J. Comput. System. Sci.*, 4:177–192, 1970.
- [9] S. Seif and C. Szabó. Computational complexity of checking identities in 0-simple semigroups and matrix semigroups over finite fields. *Semigroup Forum*, 72(2):207–222, 2006.
- [10] M. Steindl. The subpower membership problem for bands, submitted. Available at <http://arxiv.org/pdf/1604.01014v1.pdf>.
- [11] M. Steindl. *Computational Complexity of the Subpower Membership Problem for Semigroups*. PhD thesis, Johannes Kepler University Linz, Austria, 2015. Available at <http://epub.jku.at/obvulihs/download/pdf/893649?originalFilename=true>.
- [12] R. Willard. Four unsolved problems in congruence permutable varieties. Talk at International Conference on Order, Algebra, and Logics, Vanderbilt University, Nashville, June 12–16, 2007.

INSTITUTE FOR ALGEBRA, JOHANNES KEPLER UNIVERSITY LINZ, ALTENBERGER ST 69, 4040 LINZ, AUSTRIA

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COLORADO BOULDER, CAMPUS BOX 395, BOULDER, COLORADO 80309-0395

E-mail address: markus.steindl@colorado.edu